and to transmit the data received from a decoder to the main processor;

an encryption/key operation processor to convert the password to the key ("the safe key"), and then, if the secure data is not received together with the password from the safe memory interface, to transmit the safe key to the decoder and to encrypt the password with the safe key by encryption algorithm and calculate the integrity identification value of the encrypted password ("password integrity identification value") and then to transmit the password integrity identification value to a comparison/processor, and, if the secure data is received together with the password from the safe memory interface, to encrypt the secure data with the safe key and calculate the integrity identification value of the encrypted secure data ("encrypted data integrity identification value") and then to transmit the encrypted data integrity identification value together with the "encrypted data" to the comparison/processor;

a comparison/processor to transmit the stored data to the decoder if two integrity identification values are the same after comparing the "password integrity identification value" received from the encryption/key operation processor with the "password integrity identification value" stored in the data storage memory, to transmit password nonconformity to the computer and delete the temporally stored safe key on the decoder if the values are not the same, and to transmit the data to the data storage memory where "encrypted data" and "encrypted data integrity identification value" together with "password integrity identification value" are received from the encryption/key operation processor;

a data storage memory to store the encrypted data, the encrypted data integrity identification value and the password integrity identification value; and

a decoder to decode the encrypted data from the data storage memory with the safe key and then to transmit the decoded data to the safe memory interface,

a1 cont

wherein, where the said safe memory is employed, the main processor additionally has the function to transmit the password input request command to the computer system, and to transmit the password received from the keyboard to the safe memory, if the secure mode setup command received from the application program of the computer system is for the safe memory.

a2

7. (Amended) A computer secure system comprising the secure adapter, the keyboard and the computer system according to Claim 1, where a separate secure key for entering secure mode setup/clearing command is incorporated in said keyboard and/or the secure mode setup/clearing command can be created by the combination of existing key codes, the computer system has the secure key creation function, the encryption/decoding function with the secrete key and the encryption/decoding function with the secure key, and the keyboard manager with application program interface is included.

Please add the following new Claims:

a3

12. (New) The secure adapter according to Claim 2, further employing safe memory operation under the secure mode set by an application program executed in the computer system, said safe memory comprising:

a safe memory interface to transmit a password transmitted from the main processor, or the password and the data which requires security ("secure data"), to an encryption/key operation processor, and to transmit the data received from a decoder to the main processor;

an encryption/key operation processor to convert the password to the key ("the safe key"), and then, if the secure data is not received together with the password from the safe memory interface,

to transmit the safe key to the decoder and to encrypt the password with the safe key by encryption algorithm and calculate the integrity identification value of the encrypted password ("password integrity identification value") and then to transmit the password integrity identification value to a comparison/processor, and, if the secure data is received together with the password from the safe memory interface, to encrypt the secure data with the safe key and calculate the integrity identification value of the encrypted secure data ("encrypted data integrity identification value") and then to transmit the encrypted data integrity identification value together with the "encrypted data" to the comparison/processor;

a comparison/processor to transmit the stored data to the decoder if two integrity identification values are the same after comparing the "password integrity identification value" received from the encryption/key operation processor with the "password integrity identification value" stored in the data storage memory, to transmit password nonconformity to the computer and delete the temporally stored safe key on the decoder if the values are not the same, and to transmit the data to the data storage memory where "encrypted data" and "encrypted data integrity identification value" together with "password integrity identification value" are received from the encryption/key operation processor;

a data storage memory to store the encrypted data, the encrypted data integrity identification value and the password integrity identification value; and

a decoder to decode the encrypted data from the data storage memory with the safe key and then to transmit the decoded data to the safe memory interface,

wherein, where the said safe memory is employed, the main processor additionally has the function to transmit the password input request command to the computer system, and to transmit the password received from the keyboard to the safe memory, if the secure mode setup command received from the application program of

the computer system is for the safe memory.

13. (New) The secure adapter according to Claim 3, further employing safe memory operation under the secure mode set by an application program executed in the computer system, said safe memory comprising:

a safe memory interface to transmit a password transmitted from the main processor, or the password and the data which requires security ("secure data"), to an encryption/key operation processor, and to transmit the data received from a decoder to the main processor;

an encryption/key operation processor to convert the password to the key ("the safe key"), and then, if the secure data is not received together with the password from the safe memory interface, to transmit the safe key to the decoder and to encrypt the password with the safe key by encryption algorithm and calculate the integrity identification value of the encrypted password ("password integrity identification value") and then to transmit the password integrity identification value to a comparison/processor, and, if the secure data is received together with the password from the safe memory interface, to encrypt the secure data with the safe key and calculate the integrity identification value of the encrypted secure data ("encrypted data integrity identification value") and then to transmit the encrypted data integrity identification value together with the "encrypted data" to the comparison/processor;

a comparison/processor to transmit the stored data to the decoder if two integrity identification values are the same after comparing the "password integrity identification value" received from the encryption/key operation processor with the "password integrity identification value" stored in the data storage memory, to transmit password nonconformity to the computer and delete the temporally stored safe key on the decoder if the values are not the same, and to transmit the data to the data storage memory where

"encrypted data" and "encrypted data integrity identification value" together with "password integrity identification value" are received from the encryption/key operation processor;

a data storage memory to store the encrypted data, the encrypted data integrity identification value and the password integrity identification value; and

a decoder to decode the encrypted data from the data storage memory with the safe key and then to transmit the decoded data to the safe memory interface,

wherein, where the said safe memory is employed, the main processor additionally has the function to transmit the password input request command to the computer system, and to transmit the password received from the keyboard to the safe memory, if the secure mode setup command received from the application program of the computer system is for the safe memory.

14. (New) The secure adapter according to Claim 4, further employing safe memory operation under the secure mode set by an application program executed in the computer system, said safe memory comprising:

a safe memory interface to transmit a password transmitted from the main processor, or the password and the data which requires security ("secure data"), to an encryption/key operation processor, and to transmit the data received from a decoder to the main processor;

an encryption/key operation processor to convert the password to the key ("the safe key"), and then, if the secure data is not received together with the password from the safe memory interface, to transmit the safe key to the decoder and to encrypt the password with the safe key by encryption algorithm and calculate the integrity identification value of the encrypted password ("password integrity identification value") and then to transmit the password integrity identification value to a comparison/processor, and, if

the secure data is received together with the password from the safe memory interface, to encrypt the secure data with the safe key and calculate the integrity identification value of the encrypted secure data ("encrypted data integrity identification value") and then to transmit the encrypted data integrity identification value together with the "encrypted data" to the comparison/processor;

a comparison/processor to transmit the stored data to the decoder if two integrity identification values are the same after comparing the "password integrity identification value" received from the encryption/key operation processor with the "password integrity identification value" stored in the data storage memory, to transmit password nonconformity to the computer and delete the temporally stored safe key on the decoder if the values are not the same, and to transmit the data to the data storage memory where "encrypted data" and "encrypted data integrity identification value" together with "password integrity identification value" are received from the encryption/key operation processor;

a data storage memory to store the encrypted data, the encrypted data integrity identification value and the password integrity identification value; and

a decoder to decode the encrypted data from the data storage memory with the safe key and then to transmit the decoded data to the safe memory interface,

wherein, where the said safe memory is employed, the main processor additionally has the function to transmit the password input request command to the computer system, and to transmit the password received from the keyboard to the safe memory, if the secure mode setup command received from the application program of the computer system is for the safe memory.

15. (New) A computer secure system comprising the secure adapter, the keyboard and the computer system according to Claim 2, where a separate secure key for entering secure mode setup/clearing

command is incorporated in said keyboard and/or the secure mode setup/clearing command can be created by the combination of existing key codes, the computer system has the secure key creation function, the encryption/decoding function with the secrete key and the encryption/decoding function with the secure key, and the keyboard manager with application program interface is included.

A3 cont

16. (New) A computer secure system comprising the secure adapter, the keyboard and the computer system according to Claim 3, where a separate secure key for entering secure mode setup/clearing command is incorporated in said keyboard and/or the secure mode setup/clearing command can be created by the combination of existing key codes, the computer system has the secure key creation function, the encryption/decoding function with the secrete key and the encryption/decoding function with the secure key, and the keyboard manager with application program interface is included.

17. (New) A computer secure system comprising the secure adapter, the keyboard and the computer system according to Claim 4, where a separate secure key for entering secure mode setup/clearing command is incorporated in said keyboard and/or the secure mode setup/clearing command can be created by the combination of existing key codes, the computer system has the secure key creation function, the encryption/decoding function with the secrete key and the encryption/decoding function with the secure key, and the keyboard manager with application program interface is included.

18. (New) A computer secure system comprising the secure adapter, the keyboard and the computer system according to Claim 5, where a separate secure key for entering secure mode setup/clearing command is incorporated in said keyboard and/or the secure mode setup/clearing command can be created by the combination of existing key codes, the computer system has the secure key creation function,

Appendix A

5. (Amended) The secure adapter according to [any one of Claims]Claim 1 [through 4], further employing safe memory operation under the secure mode set by an application program executed in the computer system, said safe memory comprising:

a safe memory interface to transmit a password transmitted from the main processor, or the password and the data which requires security ("secure data"), to an encryption/key operation processor, and to transmit the data received from a decoder to the main processor;

an encryption/key operation processor to convert the password to the key ("the safe key"), and then, if the secure data is not received together with the password from the safe memory interface, to transmit the safe key to the decoder and to encrypt the password with the safe key by encryption algorithm and calculate the integrity identification value of the encrypted password ("password integrity identification value") and then to transmit the password integrity identification value to a comparison/processor, and, if the secure data is received together with the password from the safe memory interface, to encrypt the secure data with the safe key and calculate the integrity identification value of the encrypted secure data ("encrypted data integrity identification value") and then to transmit the encrypted data integrity identification value together with the "encrypted data" to the comparison/processor;

a comparison/processor to transmit the stored data to the decoder if two integrity identification values are the same after comparing the "password integrity identification value" received from the encryption/key operation processor with the "password integrity identification value" stored in the data storage memory, to transmit password nonconformity to the computer and delete the temporally stored safe key on the decoder if the values are not the same, and to transmit the data to the data storage memory where "encrypted data" and "encrypted data integrity identification value"

together with "password integrity identification value" are received from the encryption/key operation processor;

a data storage memory to store the encrypted data, the encrypted data integrity identification value and the password integrity identification value; and

a decoder to decode the encrypted data from the data storage memory with the safe key and then to transmit the decoded data to the safe memory interface,

wherein, where the said safe memory is employed, the main processor additionally has the function to transmit the password input request command to the computer system, and to transmit the password received from the keyboard to the safe memory, if the secure mode setup command received from the application program of the computer system is for the safe memory.

7. (Amended) A computer secure system comprising the secure adapter, the keyboard and the computer system according to [any one of Claims]Claims 1 [through 6], where a separate secure key for entering secure mode setup/clearing command is incorporated in said keyboard and/or the secure mode setup/clearing command can be created by the combination of existing key codes, the computer system has the secure key creation function, the encryption/decoding function with the secrete key and the encryption/decoding function with the secure key, and the keyboard manager with application program interface is included.